McGill Law Journal — Revue de droit de McGill

THE NEW JIM CROW: UNMASKING RACIAL BIAS IN AI FACIAL RECOGNITION TECHNOLOGY WITHIN THE CANADIAN IMMIGRATION SYSTEM

*Gideon Christian**

Despite its purported neutrality, AI-based facial recognition technology (FRT) exhibits significant racial bias. This paper critically examines the integration of FRT within the Canadian immigration system. The paper begins with an exploration of the historical evolution of AI in border control—once rooted in physical barriers—which now relies on biometric surveillance that risks replicating historical patterns of racial discrimination.

The paper further contextualizes these issues within the broader discourse of algorithmic racism, highlighting the risks of embedding historical racial injustices into AI-powered immigration systems. Drawing a parallel between FRT and Jim Crow laws that segregated and marginalized Black communities in the United States, it argues that biased FRT systems function as a modern mechanism of racial exclusion, risk denying Black and racialized immigrants access to refugee protection, and exacerbating deportation risks. It warns against the normalization of AI use in immigration decision-making without proper oversight, transparency, and regulatory safeguards.

The paper concludes by calling for enhanced government transparency and adherence to procedural fairness in the deployment of FRT within the Canadian immigration system. It further advocates for a "technological civil rights movement" to ensure that AI technologies, including FRT, uphold human rights and promote equity rather than perpetuate systemic racism.

.

Malgré sa neutralité prétendue, la technologie de reconnaissance faciale (TRF) alimentée par l'intelligence artificielle (IA) fait preuve de préjugés raciaux importants. Cet article examine critiquement l'intégration de la TRF dans le système d'immigration Canadien. Il commence avec une exploration de l'évolution historique de l'IA dans le contrôle des frontières — autrefois ancré dans les barrières physiques — qui se repose désormais sur la surveillance biométrique qui risque de reproduire les schémas historiques de la discrimination raciale.

L'article discute davantage ces questions dans le contexte plus étendu du racisme algorithmique, en soulignant les risques d'intégration des injustices raciales historiques dans les systèmes d'immigration alimentés par l'IA. En établissant un parallèle entre la TRF et les lois Jim Crow qui ségréguaient et marginalisaient les communautés noires aux États-Unis, cet article affirme que les systèmes de TRF biaisés fonctionnent comme un mécanisme moderne d'exclusion raciale qui risquent de priver les immigrants noirs et racialisés d'accès à la protection des réfugiés et d'exacerber les risques d'expulsion. Il met en garde contre la normalisation de l'utilisation de l'IA dans la prise de décision en matière d'immigration sans surveillance, transparence et garanties réglementaires adéquates.

L'article se conclut en faisant appel à une plus grande transparence gouvernementale et au respect de l'équité procédurale dans le déploiement du TRF au sein du système d'immigration Canadien. Il préconise en outre un « mouvement technologique des droits civiques » afin de s'assurer que les technologies de l'IA, y compris la TRF, respectent les droits de l'homme et favorisent l'équité au lieu de perpétuer le racisme systémique.

* PhD; Associate Professor and University Research Chair (AI and Law), Faculty of Law, University of Calgary. gideon.christian@ucalgary.ca. The author is grateful for the collaborative support provided by the Alberta Civil Liberties Research Centre (ACLRC) at the University of Calgary and for the research assistantship provided by Onyinye Odita, Karishma Akbari, Chidinma Duruiheoma, and Sabiha Meghji. Heartfelt thanks to the editors at the *McGill Law Journal* for their thoughtful review and feedback on the draft paper. This research project was funded by the Office of the Privacy Commissioner of Canada (OPC). The views expressed herein are those of the author and do not necessarily reflect those of the OPC.

Citation: (2024) 69:4 McGill LJ 441 — Référence : (2024) 69:4 RD McGill 441

Introduction

Facial recognition technology (FRT) is an artificial intelligence (AI)-based biometric technology that utilizes computer vision to analyze facial images and identify individuals by their unique facial features.[1] This sophisticated AI technology uses advanced computer algorithms to generate a biometric template from a facial image. The biometric template contains unique facial characteristics represented by dots, which can be used to match identical or similar images in a database for identification purposes. The biometric template is often likened to a unique facial signature for each individual.[2]

A significant rise in the deployment of AI-based FRT has occurred in recent years across the public and private sectors of Canadian society. Within the public sector, its application encompasses law enforcement in criminal and immigration contexts, among many others. In the private sector, it has been used for tasks such as exam proctoring in educational settings, fraud prevention in the retail industry, unlocking mobile devices, sorting and tagging of digital photos, and more. The widespread use of AI facial recognition in both the public and private sectors has generated concerns regarding its potential to perpetuate and reflect historical racial biases and injustices. The emergence of terms like "the new Jim Crow"[3] and "the new Jim Code"[4] draws a parallel between the racial inequalities of the post-US Civil War Jim Crow era and the racial biases present in modern AI technologies. These comparisons underscore the need for a critical examination of how AI technologies, including FRT, might replicate or exacerbate systemic racial inequities and injustices of the past.

This research paper seeks to examine critical issues arising from the adoption and use of FRT by the public sector, particularly within the framework of immigration enforcement in the Canadian immigration system. It delves into recent Federal Court of Canada litigation relating to the use of the technology in refugee revocation proceedings by agencies of

---

1 Gideon Christian, "#AI Facial Recognition Technology in the Retail Industry" (5 January 2023) at 1, online (pdf): <ablawg.ca> [perma.cc/EY5Z-2UMP].

2 Josh Luberisse, *Beyond the Wall: Border Security in the Age of AI and Facial Recognition Technology* (New York: Fortis Novum Mundum, 2023) at 24. Unlocking a phone with FRT involves the internal camera deploying over 30,000 "invisible" infrared dots across the face and capturing the image through the pattern created by these dots (Calvin D Lawrence, *Hidden In White Sight: How AI Empowers and Deepens Systemic Racism*, 1st ed (Boca Raton, Fla: CRC Press, 2023) at 3).

3 See e.g. Michelle Alexander, *The New Jim Crow: Mass Incarceration in the Age of Colorblindness*, 10th anniversary ed (New York: The New Press, 2020).

4 Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code* (Cambridge, UK: Polity Press, 2019) at 3.

the Canadian government.[5] By delving into these legal cases, the paper will explore the implications of FRT on the fairness and integrity of immigration processes, highlighting the broader ethical and legal issues associated with its use in administrative processes.

The paper begins with a concise overview of the Canadian immigration system and the administrative law principles applicable to its decision-making process. This is followed by an examination of the history of integrating AI technologies into the immigration process more broadly. Focusing specifically on AI-based FRT, the paper will then explore the issues of racial bias associated with its use and discuss why addressing these issues is crucial for ensuring fairness in the Canadian immigration process. This discussion will lead to a critical analysis of Federal Court litigation relating to the use of FRT in refugee status revocation, further spotlighting the evidence of racial bias in the technology's deployment within the immigration system.

The paper will then proceed to develop the parallels between racial bias evident in contemporary AI-based FRT (the "new" Jim Crow) and racial bias of the past (the "old" Jim Crow). By focusing on the Canadian immigration context, the paper seeks to uncover the subtle, yet profound ways in which AI-based FRT, despite its purported neutrality and objectivity, can reinforce racial biases of the past. Through a comprehensive analysis of current practices, judicial decisions, and the technology's deployment, this paper aims to contribute to the ongoing dialogue about technology and race. It challenges the assumption that technological advancements are inherently equitable, urging a re-evaluation of how these tools are designed, developed, and deployed, especially in sensitive areas such as refugee status revocation, where the stakes for fairness and equity are particularly high.

I. Canadian Immigration System—The Legal Framework

The primary pieces of legislation governing immigration in Canada are the *Immigration and Refugee Protection Act* (IRPA)[6] and the *Immigration and Refugee Protection Regulation* (IRPR).[7] Other operational

---

5 See *Barre v Canada (Citizenship and Immigration)*, 2022 FC 1078 [*Barre*]; *AB v Canada (Citizenship and Immigration)*, 2023 FC 29 [*AB*]; *Abdulle v Canada (Citizenship and Immigration)*, 2023 FC 162 at paras 2, 50 [*Abdulle*]; *Ali v Canada (Citizenship and Immigration)*, 2023 FC 671; *Mah v Canada (Citizenship and Immigration)*, 2023 FC 1229; *Osoble v Canada (Citizenship and Immigration)*, 2023 FC 1584; *Hassan v Canada (Public Safety and Emergency Preparedness)*, 2023 FC 1550.

6 *Immigration and Refugee Protection Act*, SC 2001, c 27 [*IRPA*].

7 *Immigration and Refugee Protection Regulation*, SOR/2002-227 [*IRPR*].

manuals and documents also provide detailed policy and procedural guidance for the interpretation of the major legislation, thus shaping the interpretation and application of the *IRPA* and *IRPR*.

The administration and enforcement of immigration regulation in Canada is overseen mainly by two federal departments/agencies: Immigration, Refugee and Citizenship Canada (IRCC), and the Canada Border Services Agency (CBSA).[8] While IRCC is responsible for processing of immigration and refugee applications allowing foreign nationals to enter or remain in Canada, the CBSA is responsible for admitting foreign nationals into Canada (at the port of entry) and enforcing their removal when their stay in Canada has ceased to be valid or they have become inadmissible.

Aside from IRCC and the CBSA, other administrative tribunals are also charged with administrative decision-making relating to immigration matters. The Immigration and Refugee Board of Canada (IRB) comprises of four administrative tribunals: the Refugee Protection Division (RPD), the Refugee Appeals Division (RAD), the Immigration Division (ID) and the Immigration Appeals Division (IAD). Generally, immigration decisions made by the IRCC, CBSA officers, and the appellate arms of the IRB tribunals, are subject to judicial review by the Federal Court of Canada, and in some specific cases,[9] they are subject to further appeal to the Federal Court of Appeal and the Supreme Court of Canada.

Immigration decisions by IRCC and CBSA officers and the IRB tribunals fall within the context of administrative decision-making processes.[10] Hence, these decisions must adhere to the principles of administrative law, notably the principle of procedural fairness, which is fundamental to the Canadian legal framework and applicable across a variety of legal and

---

8 Employment and Social Development Canada (ESDC) also plays some role in the administration and enforcement of immigration laws in Canada, particularly those related to the labour market and employment of foreign nationals, such as the processing and issuance of Labour Market Impact Assessments (LMIA).

9 Judicial review decisions of the Federal Court can only be appealed to the Federal Court of Appeal if the Federal Court, in rendering its decision, certifies a question. A certified question is a question of serious general importance certified by the court in accordance with *IRPA*, *supra* note 6, s 74 or *Citizenship Act*, RSC 1985, c C-29, s 22.2 (see *Mason v Canada (Citizenship and Immigration)*, 2023 SCC 21 at paras 49–52). See also Steven Meurrens, "Certified Questions and the Federal Court of Appeal" (13 July 2018), online (blog): <meurrensonimmigration.com> [perma.cc/9XH4-B654].

10 See *Mubiayi v Canada (Citizenship and Immigration)*, 2017 FC 1010 at paras 6–10. As a matter of fact, the IRB is "Canada's largest independent administrative tribunal" (see Immigration and Refugee Board of Canada, "About the Board" (last modified 23 April 2024), online: <irb-cisr.gc.ca> [perma.cc/5PGV-MXQN]).

administrative proceedings, including those in immigration.[11] In the administrative context, the principle requires that decisions made by administrative officers must be based on evidence, be free from bias, and follow the principles of justice and equity. Such decisions should be made transparently and be logically connected to the evidence presented.[12] Procedural fairness also encompasses the right of individuals to be informed about the decisions made regarding their case, including being provided with reasons for decisions (especially negative decisions), and how the decision-maker arrived at the decision. The reasons enables the person affected by the decision to understand its basis and, if necessary, to challenge it through appeals or judicial review.[13]

Procedural fairness is crucial for ensuring that the immigration process is just, equitable, and transparent. It ensures that individuals affected by immigration decisions have clear avenues to seek redress, thereby reinforcing the integrity and trust in the system's operations. Hence, the principle of procedural fairness becomes more crucial in the immigration context in Canada because of the wide discretion accorded to immigration decision-makers.[14] Procedural fairness helps to curtail "arbitrary, unfair, or unaccountable decision-making in situations with significant consequences for people's lives."[15] The degree of procedural fairness accorded to an individual increases or decreases with the impact the decision may have on the affected individual.[16] For example, the degree of procedural fairness owed to a temporary residence visa applicant will usually be lower than that owed to a refugee claimant. This difference is because the impacted rights from a failed refugee claim has more serious consequences compared to a failed temporary residence visa application, especially a failed refugee claim may raise the claimant's risk of deportation—with significant consequences to their right to life, liberty, and personal security.[17]

Also, related to procedural fairness is the right to be heard. In the immigration context, Molnar and Gill have noted that this right requires

---

11 See *Darwisheh v Canada (Citizenship and Immigration)*, 2024 FC 98 at paras 13–15.

12 *Sopeyin v Canada (Citizenship and Immigration)*, 2023 FC 1435 at para 25.

13 *Baker v Canada (Minister of Citizenship and Immigration)*, 1999 CanLII 699 (SCC) at para. 21.

14 *Zhang v Canada (Minister of Citizenship and Immigration)*, 2003 FC 1493 at para 7.

15 Petra Molnar & Lex Gill, *Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System* (Toronto: Citizen Lab & International Human Rights Program, 2018) at 47.

16 *Ibid* at 48.

17 *Canadian Charter of Rights and Freedoms*, s 7, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 [*Charter*].

that when a decision-maker relies on extrinsic evidence in arriving at a decision, the individual affected by the decision must be informed of such evidence and also be given the opportunity to respond accordingly.[18] This right is also implicated in situations where an immigration officer relies on an AI algorithm in arriving at a decision.[19] Hence, individuals affected by such decisions ought to be made aware of the decision-maker's reliance on the AI tool and be given the opportunity to challenge the decision made by, or with the help of this technology.

II. Historical Perspective: How AI Has Been Integrated into Immigration Processes

In his work, Luberisse discusses how physical barriers like walls played a crucial role in deterring invasions, regulating trade, and managing migration flows – prior to the development of sophisticated border control technologies.[20] He supports this assertion with notable historical examples, such as the Great Wall of China, which was built to safeguard Chinese states from nomadic invasions, and Hadrian's Wall in Northern England, representing the boundary of the Roman Empire.[21] These structures were more than mere defensive strategies as they also fulfilled exclusionary functions – excluding undesirable elements from defined spaces, such as territorial boundaries. These examples are illustrative of the multifaceted roles of physical barriers in the annals of history.

Over time, paper passports containing the facial image of the holder have evolved to become essential documents for countries to regulate immigration flows and verify the identities of travellers seeking to enter their territorial spaces.[22] Traditionally, this verification process involved border officers manually comparing the photo image on the passport document with the traveller's face. This method, while straightforward, could be time-consuming and prone to human error, highlighting the need for more efficient and reliable verification techniques.[23]

With the development of pertinent technology over the late 20th and early 21st centuries, a significant shift has emerged towards the use of more sophisticated systems in immigration processes. The development of AI and machine learning algorithms offered unprecedented capabilities

---

18 Molnar & Gill, *supra* note 15 at 49.

19 *Ibid*.

20 Luberisse, *supra* note 2 at 1.

21 *Ibid* at 1–2.

22 *Ibid* at 34.

23 *Ibid* at 32.

for data analysis, pattern recognition, and automation. Governments and immigration authorities began to see that technologies had the potential to not only transform traditional processes, but also to become useful tools that streamline the process by enabling quicker and more accurate adjudications of immigration applications, border control procedures, and identity verification.

The advent of biometric technology, including fingerprint and facial recognition, marked a crucial point in the deployment of sophisticated technologies in immigration processes. Initially used for security and verification purposes, these technologies have become increasingly central to immigration controls, aiding in identifying and tracking individuals as they seek to cross national borders, and even when they enter spaces within a sovereign state.

In Canada and the United States, we are witnessing the increasing use of AI in border and immigration systems.[24] This trend represents a significant shift towards more efficient, secure, and intelligent management of the immigration system. In the United States, the US Custom and Border Protection (CBP) has deployed AI-driven FRT across US airports and border crossings to enhance the screening process of incoming and outgoing travellers.[25] This system, which is part of the Biometric Entry-Exit Program,[26] aims to verify identities quickly and accurately, reducing wait times and increasing security by identifying individuals who may pose a security risk, or have overstayed their visas.

In Canada, the IRCC employs advanced analytics and machine learning algorithms to sift through and triage large volumes of immigration applications.[27] This application of AI helps to identify patterns that may indicate fraudulent documents or applications, thereby enhancing the vetting process and prioritizing cases that require closer human examination. IRCC has also deployed Chinook software to improve efficiency and

---

[24] Gideon Christian, "AI Facial Recognition Technology in the Canadian Immigration System", *Canadian Immigration Lawyers Association* (29 August 2023), online (blog): <cila.co> [perma.cc/C499-J7C5]. See also Hannah Tyler, "The Increasing Use of Artificial Intelligence in Border Zones Prompts Privacy Questions", *Migration Policy Institute* (2 February 2022), online: <migrationpolicy.org> [perma.cc/PT4X-UXTH].

[25] Davey Alba, "The US Government Will Be Scanning Your Face At 20 Top Airports, Documents Show", *BuzzFeed News* (11 March 2019), online: <buzzfeednews.com> [perma.cc/D9QE-4VBW].

[26] US Customs and Border Protection, "Say Hello to the New Face of Efficiency, Security and Safety: Introducing Biometric Facial Comparison Technology" (last modified 3 September 2024), online: <cbp.gov> [perma.cc/3QWY-JNL8].

[27] See Immigration, Refugees and Citizenship Canada, "CIMM – Question Period Note – Use of AI in Decision-Making at IRCC – November 29, 2022" (last modified 28 March 2023) online: <canada.ca> [perma.cc/8DEM-KQ2Q].

processing times for temporary residence application.[28] As we will see later, it appears that the department has also deployed the use of AI-based FRT in identity verification of refugee claimants in Canada.[29]

Similarly, CBSA has deployed Primary Inspection Kiosks or eGates, and NEXUS kiosks across major airports in Canada.[30] These kiosks use AI-based FRT to verify the identity of persons seeking to enter Canada and expedite their customs declaration process. The process involves face verification: a one-to-one photo comparison.[31] The traveller arriving at the kiosks will have their photo taken and ePassport document scanned.[32] The photo image taken at the kiosk is then used by the FRT system to generate a unique biometric template of the individual, which is subsequently matched against the photo embedded in the chip of the traveller's ePassport or, in the case of a NEXUS travellers, against the digital photo archived in the CBSA systems.[33] This process ensures that the two images match. Implementing this technology offers an extra layer of verification using the traveller's facial image, thereby enhancing travel security and recognizing the traveller's eligibility for entry into Canada. Luberisse noted that FRT systems "are revolutionizing border security propelling it into an era where identification is not just about documents but the very essence of human biology."[34]

III. Racial Bias in AI Facial Recognition Technology

Andrejevic and Selwyn have pointed out that a recurring fault line in the historical development of FRT is its complete failure to engage with

---

[28] See especially Immigration, Refugees, and Citizenship Canada, "CIMM — Chinook Development and Implementation in Decision-Making – February 15 & 17, 2022" (last modified 10 May 2022), online: <canada.ca> [perma.cc/HX55-WSWQ]. While many immigration lawyers have consistently asserted that Chinook is an AI-based software, the IRCC, on the other hand, has maintained that the software is a Microsoft Excel-based tool and not an AI-based tool and thus has no built-in decision-making algorithm (see also *Ocran v Canada (Citizenship and Immigration)*, 2022 FC 175 at para 57 [*Ocran*]).

[29] *Barre*, *supra* note 5 at para 46.

[30] Canada Border Services Agency, "Smart and Secure Border Tools for Travel and Trade" (last modified 15 April 2024), online: <cbsa-asfc.gc.ca> [perma.cc/485Q-A3K8].

[31] This is different from face identification which involves one-to-many (1:n) photo comparison.

[32] Canada Border Services Agency, "Declare Your Travel Information at an Airport Kiosk or eGate: How to Use the Kiosks and eGate" (last modified 1 October 2022), online: <cbsa-asfc.gc.ca> [perma.cc/CD7X-YM62].

[33] Alyssa Herage, "Facial Verification at the Border", *Canada Border Services Agency* (4 June 2021), online: <publicsafety.gc.ca> [perma.cc/9HGE-DHDK].

[34] Luberisse, *supra* note 2 at 31.

issues of race and racism.[35] That early historical trend set a negative precedent, leading to the modern incarnation of the technology, which is profoundly entangled with racial bias. According to Andrejevic and Selwyn, that trend "tended to lead white middle-aged researchers to seek out datasets populated with pictures of faces fitting the white, middle-aged profile of what they deemed to be 'Mr Average'.[36] Further, many research studies have consistently demonstrated that while FRT exhibits a high accuracy rate in recognizing faces with lighter skin tones, it exhibits high error rates in identifying faces with darker skin tones.[37] These widely divergent accuracy rates of FRT along racial lines unquestionably bring the technology's evident racial bias into clear focus. This disparity underscores a significant challenge in ensuring the technology's fairness and accuracy across diverse racial demographics.

Buolamwini and Gebru's landmark Gender Shades study exposed significant racial and gender biases within commercial facial analysis algorithms.[38] Their research made clear that the datasets used to train these systems predominantly feature White male individuals, leading to a skewed representation that affects the algorithms' accuracy in identifying and classifying individuals by gender and skin colour.[39] The findings revealed a pronounced bias against darker-skinned females, who experienced identification error rates as high as 34.7%.[40] In contrast, lighter-skinned males had an error rate as low as 0.8%, indicating a 99.2% accuracy rate for this group.[41]

This study builds on earlier research by Klare et al., who conducted a large-scale analysis of facial recognition performance across three demographic classifications: race/ethnicity, gender, and age.[42] This analysis, which evaluated the results from three commercial facial recognition algorithms, consistently found lower accuracy rates among females and

---

35 Mark Andrejevic & Neil Selwyn, *Facial Recognition* (Cambridge, UK: Polity Press, 2022) at 15.

36 *Ibid*.

37 Joy Buolamwini & Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification" (2018) 81 Proceedings Machine Learning Research 1 at 10; Alex Najibi, "Racial Discrimination in Face Recognition Technology" (24 October 2020) online (blog): <sitn.hms.harvard.edu> [perma.cc/V5LA-S56D].

38 Buolamwini & Gebru, *supra* note 37 at 10.

39 *Ibid* at 7

40 *Ibid* at 8, 11.

41 *Ibid* at 9.

42 Brendan F Klare et al, "Face Recognition Performance: Role of Demographic Information" (2012) 7:6 IEEE Transactions on Information Forensics & Security 1789 at 1789.

Black individuals aged 18 to 30 years.[43] Together, these studies underscore the critical need to address and rectify the biases inherent in facial recognition technologies, while shining a light on the disparities in accuracy that disproportionately affect certain demographic groups.

The U.S. National Institute for Standards and Technology (NIST) conducted a comprehensive study to evaluate the impact of race, gender, and age on the accuracy of facial recognition software.[44] This study, one of the most extensive of its kind, evaluated 189 facial recognition software systems from 99 developers, representing a significant portion of the industry. It employed two testing methods: one-to-one (1:1) photo matching (face verification) and one-to-many (1:n) photo matching (face identification). The findings revealed a higher incidence of false positives in face verification tests for West and East African faces compared to East European faces, and for East Asian faces compared to East European faces, specifically when algorithms were tested using higher-quality application photos. Additionally, the study noted that for U.S. domestic law enforcement images, American Indian faces exhibited higher false positive rates than both West and East African and East Asian faces. Moreover, it highlighted that Chinese-developed algorithms demonstrated low false positive rates for East Asian faces.[45] In face identification tests, the study observed an increased rate of false positives specifically among Black females.[46]

Similarly, the UK-based National Physical Laboratory undertook independent testing of facial recognition software utilized by two major UK police departments.[47] This testing indicated that the software's performance was particularly poor regarding Black females.[48] This bias existed despite these police departments' efforts to implement an Equality Impact Assessment process designed to prevent unlawful discrimination result-

---

43 *Ibid* at 1800.

44 See generally Patrick Grother, Mei Ngan & Kayee Hanaoka, *Face Recognition Vendor Test Part 3: Demographic Effects*, NISTIR 8280 (National Institute of Standards and Technology, 2019).

45 *Ibid* at 2, 7. See also K S Krishnapriya et al, "Characterizing the Variability in Face Recognition Accuracy Relative to Race" (paper delivered at the 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, 16-20 June 2019) [unpublished], which was cited in the NISTIR 8280.

46 Grother, Ngan & Hanaoka, *supra* note 44 at 63. See also National Institute of Standards and Technology, "NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software" (19 December 2019), online: <nist.gov> [perma.cc/M2SZ-SX3K].

47 Metropolitan Police Service (MPS) and South Wales Police (SWP).

48 Tony Mansfield, *Facial Recognition Technology in Law Enforcement Equitability Study*, NPL Report MS 43 (Middlesex: NPL Management Limited, 2023) at 20.

ing from the technology's use.[49] In a court ruling in *R. (Bridges) v Chief Constable of South Wales*, the Court of Appeal of England and Wales found the police department's Equality Impact Assessment and their overall approach failed to sufficiently mitigate the risk of racial bias in the deployment of automatic FRT.[50]

Thus, most available research studies clearly suggest that facial recognition software appears to exhibit higher error rates among people of colour, the highest rate occurring among Black females. The consequences of false positives in face identification can be profound, especially in public sector applications of the technology. For instance, when an individual's image is used to search a broader database within contexts such as immigration or criminal justice enforcement, the repercussions of inaccuracies could be critical, affecting lives and potentially leading to unjust outcomes. The potential for errors underlines the urgent need for addressing these disparities to ensure fairness and accuracy in the application of FRT.

Aside from the racial bias evident in these studies, other studies have even gone further, drawing attention to the high error rate in the technology more broadly. For example, in 2019, Manthorpe and Martin noted that 81% of persons flagged by the live FRT used by the London Metropolitan Police Service were falsely flagged as suspect—raising significant concern about the police use of the technology.[51] Even in cases where research studies have reported an overall high FRT accuracy rate, this accuracy rate may be misleading: once it is actually broken down along racial and gender lines, a different picture becomes apparent.[52] These kinds of deeper analysis will inevitably reveal the racial and gender bias imbedded in the technology. Therefore, even where the overall predictive ac-

---

49 See Metropolitan Police, "Equality Impact Assessment" (last accessed 13 March 2024) at 2, online (pdf): <met.police.uk> [perma.cc/P55K-XQ58].

50 See *R (Bridges) v Chief Constable of South Wales Police*, [2020] EWCA Civ 1058 at 173–202.

51 Rowland Manthorpe & Alexander J Martin, "81% of 'Suspects' Flagged by Met's Police Facial Recognition Technology Innocent, Independent Report Says" (4 July 2019), online: <news.sky.com> [perma.cc/Y5EA-EHER]. Fussey and Murray reviewed six test deployments of facial recognition technology by the Metropolitan Police Service between 2016 and 2019. The technology generated 46 matches involving 45 separate persons. The accuracy rate across all deployments was 19.05% (see Pete Fussey & Daragh Murray, *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, The Human Rights, Big Data and Technology Project (Essex: University of Essex Human Rights Centre, 2019) at 10).

52 For the 97.35% reported accuracy rate, see Yaniv Taigman et al, "DeepFace: Closing the Gap to Human-Level Performance in Face Verification" in *2014 IEEE Conference on Computer Vision and Pattern Recognition* (Conference Publishing Services, 2014), 1701–08.

curacy of FRT tools may appear high, users must remember that some racial groups are disproportionately impacted by its predictive inaccuracy. This issue is evident from highly publicized cases of false arrests arising from false positive matches by the software.

In the United States, there have been six documented instances of false arrests attributed to the use of FRT by police departments.[53] Remarkably, all these cases involved individuals who are Black. Notably, half of these incidents occurred in Detroit. This city is known for Project Green Light, a program that extensively employs CCTV cameras and FRT for public surveillance. Given that Detroit's population is over 77.8% Black,[54] these incidents raise significant concerns about the appropriateness of deploying a technology proven to have its highest error rates among this demographic group.[55] This pattern emphasizes the critical need to re-evaluate the use of FRT by law enforcement, particularly in areas with high concentrations of populations most susceptible to its inaccuracies.

IV. Deportation 2.0: AI Facial Recognition Technology in the Canadian Immigration System

Canada has been at the forefront of integrating AI technologies into its immigration and border control systems. This AI technology adoption has often been covert, with the public only learning about the use of spe-

---

53 (1) Robert Williams: see Kashmir Hill, "Wrongfully Accused by an Algorithm", *The New York Times* (24 June 2020), online: <nytimes.com> [perma.cc/AH9Z-AE3L]; (2) Michael Oliver: see Drew Harwell, "Wrongfully Arrested Man Sues Detroit Police Over False Facial Recognition Match", *The Washington Post* (13 April 2021), online: <washingtonpost.com> [perma.cc/3RKS-F6KD]; (3) Nijeer Parks: see John General & Jon Sarlin, "A False Facial Recognition Match Sent This Innocent Black Man to Jail", *CNN* (19 April 2021), online: <cnn.com> [perma.cc/SH5D-8WPF]; (4) Randall Reed: see Josh Marcus, "Louisiana Police Sued for Wrongly Arresting Black Man Using AI Face Recognition Programme", *The Independent* (26 September 2023), online: <independent.co.uk> [perma.cc/8D4W-J3SW]; (5) Alonzo Sawyer: see Khari Johnson, "Face Recognition Software Led to His Arrest. It Was Dead Wrong", *Wired* (28 February 2023), online: <wired.com> [perma.cc/359R-K72H]; (6) Porcha Woodruff: see Raymond Strickland, "Detroit Woman at Center of Facial Recognition Lawsuit Responds to Police Chief's Claims", *CBS News* (10 August 2023), online: <cbsnews.com> [perma.cc/LVZ3-HKGH].

54 United States Census Bureau, "QuickFacts: Detroit City, Michigan; United States" (last accessed 13 March 2024), online: <census.gov> [perma.cc/MQ48-FRDT].

55 James Craig, the former Detroit Police Chief was quoted as saying: "If we were just to use the technology by itself, to identify someone, I would say 96 percent of the time it would misidentify" (Jason Koebler, "Detroit Police Chief: Facial Recognition Software Misidentifies 96% of the Time", *Vice Media* (29 June 2020), online: <vice.com> [perma.cc/CGQ2-KW2M]).

cific AI technologies in immigration processes either through litigation[56] or via access to information requests made by private citizens. Judicial reviews from the Federal Court have shed light on the Government of Canada's use of FRT in immigration enforcement, illuminating numerous issues and concerns in this process. These concerns include racial bias, procedural fairness, and transparency, reflecting the complexities and challenges of integrating AI into sensitive governmental operations. This insight underscores the need for more transparency and scrutiny with respect to the deployment of AI technologies in public sector domains, particularly in areas as critical as immigration and border security.

The general tendency of AI tools to exhibit racial bias has been referred to as "algorithmic racism," defined in a previous work as "systemic, race-based bias arising from the use of AI-powered tools in ... decision making resulting in unfair outcomes to individuals from a particular segment of the society distinguished by race."[57]

Principles of administrative law require administrative decision-making processes to be free of bias, including racial bias. This principle assumes even greater importance when AI tools are integrated into such decision-making. As Calvin Lawrence has pointed out, if AI tools are designed without sufficiently addressing existing biases and inequities, the biases embedded within the algorithms can compromise the integrity of predictive decisions, leading to subtle forms of discrimination that may not be immediately apparent.[58]

Hence, where an AI tool that has been proven to exhibit racial bias is used in an administrative decision-making process, a pervasive risk exists that the decision arising from that process will be tainted by bias—unless of course the decision-maker can account for the bias.[59] Regarding the use of FRT in the Canadian immigration system, a review of Federal Court litigation related to its use suggests not only racial bias that decision-makers could not account for, but also a clear lack of transparency and procedural fairness, further evidencing systemic racism.

---

56 For example, the use of Chinook software in the processing of immigration applications by IRCC was a closely guarded secret until the *Ocran* case (see *Ocran*, *supra* note 28). See also *Barre*, *supra* note 5.

57 Gideon Christian, "Artificial Intelligence, Algorithmic Racism and the Canadian Criminal Justice System" (26 October 2020), online (blog): <slaw.ca> [perma.cc/2FVB-F6JR].

58 See Lawrence, *supra* note 2 at 33.

59 For example, the bias could be accounted for by attaching little or no weight to the prediction made by the AI tool, or the decision-maker could seek additional evidence to collaborate the evidence from the AI tool.

To understand the depth of these issues, it is instructive to examine specific Federal Court litigation, beginning with *Barre v. Canada (Citizenship and Immigration)*.[60] This case, among others, highlights the critical concerns about the use of such technology and its impact on fairness and equality in administrative decision-making processes, particularly in sensitive areas like immigration, where the stakes are high for the individuals involved. *Barre* was the first Canadian litigation that alerted the Canadian public to the use of FRT in the context of immigration enforcement. The case raised allegations regarding its usage in refugee status revocation by the Minister of Public Safety and Emergency Preparedness, represented by two government departments, IRCC and CBSA.

The applicants were two Somali women who had previously made successful refugee claims in Canada. Subsequently, the Minister of Public Safety and Emergency Preparedness successfully brought an application for the revocation of their refugee status before the Refugee Protection Division (RPD). The minister alleged that the women had misrepresented their identity as Somali nationals when, in fact, they were Kenyan citizens. It appeared that IRCC had matched the facial photos of the women with those of two different individuals who were Kenyan nationals and who had previously entered Canada with Kenyan passports. While the RPD accepted evidence of the photo match, it refused the women's request to compel the minister to disclose information about the technology used in the photo comparison.

At the judicial review of the RPD decision at the Federal Court, the applicants asserted that the minister used the controversial Clearview AI-based FRT in the photo-matching process.[61] Thus, the use of an FRT tool in the administrative judicial decisions that led to the refugee status revocation became a major issue in the litigation. This issue was critical for several reasons: First, FRT is known for its high error rate in identifying Black women, a racial and gender group to which these women belong, raising critical concerns about accuracy and bias in the impugned revocation decision. Second, given FRT's high error rates and the potential for inherent bias, it is crucial to examine the measures the immigration officers took to address the inherent bias in this revocation decision. Third, the applicants' unsuccessful efforts to obtain disclosure from the immigration authorities about the use of the technology are certainly cause for concern about procedural fairness in the decision-making process.

---

60 *Barre*, *supra* note 5.

61 Interview of Hoan Ton-That by Donie O'Sullivan (2020) on *CNN*, online: <cnn.com> [perma.cc/Y59C-LZQP].

The judicial review of the IRCC's revocation decision in *Barre* made evident a significant lack of transparency on the government's part. The minister attempted, albeit unsuccessfully, to evade the issue of disclosing the technology used in photo matching by invoking Section 22(2) of the *Privacy Act*.[62] The minister argued that the provision "allows law enforcement agencies to protect the details of [their] investigation."[63] Essentially, the minister argued that the technology employed for photo matching was an "investigative technique" and therefore exempt from disclosure. Beyond asserting the use of FRT in the photo matching, the applicants presented empirical evidence and research studies to the Federal Court, demonstrating the technology's high error rates in identifying darker-skinned females like themselves. In its decision, the Federal Court accepted that FRT was used in the photo matching. It determined that the minister could not rely on Section 22(2) of the *Privacy Act* to avoid disclosing information about its application. Citing reports from the "Gender Shades" study, the court acknowledged the applicants' characterization of FRT as an unreliable pseudoscience, one that "has consistently struggled to obtain accurate results, particularly with regard to Black women and other women of colour."[64]

If we accept the Federal Court's finding that FRT was used by immigration officials in the photo matching, this case raises some serious questions. First, why was the use of this technology in the decision-making process not disclosed to the applicants? Why did the minister oppose the disclosure of information relating to its usage at all stages of the proceedings? But even more critically—given the overwhelming evidence of racial and gender biases against darker-skinned females associated with FRT—why would a government department deploy such technology in an administrative decision-making process affecting individuals from racial and gender groups known to be adversely affected by FRT biases? One might be inclined to suggest that these known issues with FRT could explain the minister's opposition to disclosure. One interpretation is that invoking the *Privacy Act* was an attempt by the minister to avoid scrutiny over numerous issues related to the use of the technology in government administrative decision-making. Unfortunately, due to the nature of judicial review litigation, these concerns were not, and could not have been, addressed by the Federal Court, as the matter was returned to the RPD for redetermination.

---

62 RSC 1985, c P-21, s 22(2).

63 *Barre*, *supra* note 5 at para 7.

64 *Ibid* at para 25.

Given the issues raised in *Barre*, along with both the court's decision in that case and the well-documented research works and reports highlighting the bias in FRT, it is reasonable to expect that the Canadian immigration officials would rethink and revisit their use of the technology in refugee revocation proceedings involving Black people and people of colour. Sadly however, *Barre* was the first but not the last such case. Shortly after the decision in *Barre*, many other cases began to emerge from the Federal Court. One of those cases was *Abdulle v. Canada (Citizenship and Immigration)*.[65] The facts in *Abdulle* were very similar to *Barre*. It also involved a Somali female who made a successful refugee claim in Canada, and whose status was sought to be revoked because her face was matched to some other person of Kenyan nationality in the immigration database.[66] The outcome in *Abdulle* was different, though, based more on a technicality than on substantive issues.[67]

In contrast to the *Barre* case, where the appellant at least sought (albeit unsuccessfully) the disclosure of the technology behind the photo comparison, *Abdulle* did not seek disclosure at the RPD. During the Federal Court's judicial review of the RPD's revocation decision, the applicant posited that the minister must have used Clearview's AI-based FRT to compare her face against millions of others in the database. The omission to seek disclosure at RPD was ultimately fatal to the case, as the applicant's claim about the alleged use of FRT by the immigration authorities was held by the court to be speculative in the absence of any evidence. That notwithstanding, the Federal Court clearly acknowledged the weakness with FRT, stating that "the weaknesses of facial recognition software are common knowledge."[68] Thus, that "common knowledge" would have helped the applicant's case if they had sought disclosure of evidence to substantiate their claim relating to the use of the technology.

Although *Abdulle* failed on this technicality, the case further showed the lack of transparency that characterizes the questionable deployment of racially biased FRT on refugee status revocation involving Black individuals, especially Black women. Similar to *Barre*, the immigration authorities in *Abdulle* were not forthright about the use of the FRT in the photo matching. The minister denied using Clearview's FRT and instead asserted that it used "traditional investigation techniques."[69] This is problematic and deliberately confusing. First, the minister's denial relates to

---

65 *Supra* note 5.

66 *Ibid* at paras 16, 18.

67 *Ibid* at para 53.

68 *Ibid* at para 35.

69 *Ibid* at para 27.

the use of a specific *brand* of FRT—Clearview—as opposed to denial of use of FRT generally. Second, the minister asserted that it used "traditional investigation techniques," a term that appears to have been deliberately coined to conceal the disclosure of the *particular* technology used, thereby evading the scrutiny arising from the use of a clearly racially biased tool. In response, the Federal Court noted the ambiguity of the coded phrase "traditional investigation techniques," stating that "[w]hatever those techniques were, no inference can be drawn that they included facial recognition software in the absence of supporting evidence."[70] Unfortunately, the supporting evidence necessary to make the inference had been deliberately withheld by the government.

Prior to *Abdulle*, there was the case of *AB v. Canada (Citizenship and Immigration)*, involving the use of facial recognition evidence in refugee revocation.[71] This case was problematic in many respects. In addition to the issue of lack of transparency that has become characteristic of the current immigration authorities' use of FRT, *AB* also foregrounded an issue of privacy arising from the transfer of personal information collected via FRT between various levels of government. Notably, this information transfer is conducted without the knowledge or consent of the affected individual.

The applicant in *AB* was a Black woman from Central Africa who had made a successful refugee claim in Canada. Many years after her successful refugee claim, she visited an Ontario Ministry of Transportation (MTO) registry office to have her photo taken as part of her driver's licence application. Unbeknownst to her, an MTO agent used FRT to compare her photo against other photos is their database, matching her face to a different person. MTO, a *provincial* government ministry, covertly shared this information with IRCC,[72] which successfully brought a refugee revocation application at the RPD. During the RPD proceedings, the

---

70 *Ibid* at para 34.

71 *AB*, *supra* note 5 at paras 10–11.

72 During the course of the research for this paper, and upon becoming aware of the sharing of information by the MTO with IRCC, the author made a freedom of information request to the MTO in an effort to determine whether the transfer of information to IRCC was based on any existing information-sharing agreement between the government of Ontario and the federal government. The only agreement disclosed from the request was dated the 20th day of July, 1983, between the Government of Canada and the Government of the Province of Ontario to "provide for access to, and the use and disclosure of personal information under the control of a government institution **to** Ontario or a provincial institution for the purpose of administering or enforcing any law or carrying out a lawful investigation pursuant to paragraph 8(2)(f) of the Privacy Act" [Emphasis added]. In the absence of any other information sharing agreement existing between the province and the federal government, it is doubtful if the transfer of Ms. AB's information can be justified under this agreement.

applicant sought to have the MTO official testify about the ministry's use of FRT in the photo matching. IRCC successfully opposed the move.

The consistent efforts by Canadian immigration authorities to oppose the disclosure of information related to the use of FRT in immigration proceedings are very troubling, especially when this deployment involves individuals from racial and gender groups who are particularly adversely impacted by the technology's bias. AI technology is essentially a "black box;" as such, it is only common sense that in an administrative decision-making process, which should most certainly be characterized by transparency, using such opaque technology be subject to necessary scrutiny rather than shrouded in secrecy. The principle of procedural fairness demands that individuals who are affected by administrative decisions made with the assistance of AI tools, such as FRT, should be informed about the technology's role in key decisions that have lasting real-life consequences for them. Such disclosure is necessary to enable them to exercise their right to challenge those decisions.

AI-based FRT is far from neutral and free of bias. In fact, when it comes to accuracy rates and bias, FRT clearly ranks as the worst of all biometric technologies.[73] Its role in reinforcing systemic and historical racism within society is a topic that continues to be extensively researched and documented. The need for further research in this area is increasingly imperative. Hence, this study aims to augment the expanding body of research in this area. In the absence of rigorous oversight, FRT poses the risk of perpetuating the very forms of systemic racism that society has endeavoured to overcome. This trajectory becomes more apparent when we examine certain characteristics that FRT shares with the systemic racism of the past.

V. Facial Recognition Technology as the New Jim Crow

Jim Crow is a pejorative term derived from a popular American theatrical show and was used to stereotypically depict African Americans. Jim Crow laws were a series of state and local regulations that enforced racial segregation primarily, but not exclusively, in southern and border states of the United States from the late 19th century until the mid-20th century.[74] These laws and regulations deprived African Americans of many

---

[73] Trenton W Ford, "It's time to address facial recognition, the most troubling law enforcement AI tool", *Bulletin of Atomic Scientists* (10 November 2021), online: <thebulletin.org> [perma.cc/5TPJ-TYUS]. Other biometric technologies include voice recognition, retina scan, fingerprint recognition, iris recognition, DNA matching, etc.

[74] Jim Crow Museum, "What Was Jim Crow" (last accessed 13 March 2024), online: <jimcrowmuseum.ferris.edu> [perma.cc/9JHL-EUS5].

rights and excluded them from certain spaces.[75] Jim Crow laws were primarily rooted in the broader theme of systemic racial discrimination. They were a form of institutionalized racial discrimination that sought to maintain White supremacy and control over Black populations. The well-documented racial bias in FRT in many ways mirrors the ugly Jim Crow laws of the past. In the context of modern technology, racial bias in FRT represents a continuation of the systemic racial issues that characterized the Jim Crow era, albeit in a different form.

A. Spatial and Temporal Exclusion

One of the most evident manifestations of Jim Crow laws was the systematic exclusion of Black individuals and people of colour from specific public spaces, such as schools, transportation systems, restrooms, and restaurants.[76] Even in spaces where outright exclusion did not apply (such as in public buses and cinemas), these racial groups were often relegated to the most inferior segments within those spaces.[77] However, the ramifications of Jim Crow laws extend far beyond their immediate spatial restrictions, to encompass the temporal: they endured through time, well after they were officially repealed. These enduring and significant impacts are found in ongoing systemic inequalities, particularly within the criminal justice space, where Black people and people of colour are disproportionately over-represented. The socio-economic barriers and structures that were established during the Jim Crow era continue to hinder the full participation of these groups in societal progress, illustrating how the legacy of Jim Crow laws transcends both space and time.[78]

Similar to the exclusionary practices of the Jim Crow era, FRT has the potential to act as a modern instrument of exclusion.[79] This issue is

---

75 Jim Crow Museum, "Sitting for Justice" (last accessed 13 March 2024), online: <jimcrowmuseum.ferris.edu> [perma.cc/NG6E-CNAJ].

76 Jim Crow Museum, *supra* note 74.

77 On November 8, 1946, Viola Desmond, an African Canadian businesswoman, was arrested in New Glasgow, Nova Scotia, for sitting in the main floor section of the theatre. The main floor was designated as "Whites-Only," while Black patrons were relegated to the Balcony section (Parks Canada, "Viola Desmond National Historic Person (1914–1965)" (last modified 14 January 2025), online: <parks.canada.ca> [perma.cc/RC54-335S]); see also "Segregation in Transportation: Substantive and Remedial Problems" (1956) 31:2 Ind LJ 286 at 288.

78 Alexander, *supra* note 3 at 223.

79 Madison Square Garden (MSG) Entertainment had used FRT deployed on its event place in New York to prevent lawyers affiliated with law firms involved in litigation against the corporation from attending events held at Madison Square Garden. Although this exclusion was not based on race, it serves to illustrate the exclusionary capabilities of the technology (Kashmir Hill & Corey Kilgannon, "Madison Square Gar-

especially true in scenarios where access to certain benefits hinges on the accurate facial identification of individuals. The technology's demonstrated accuracy rate of over 99% in identifying White male faces suggests that individuals from this demographic are more likely to access such benefits. Conversely, individuals from racial groups that the technology struggles to accurately recognize are at a higher risk of being excluded from such benefits.

To illustrate, in Canada, both domestic and international laws recognize the right to grant refugee status to individuals fleeing persecutions from other countries. The grant of this critical status is dependent on identity verification of the claimant. However, if such verification relies on a technology notorious for its high error rates in recognizing Black individuals and people of colour, we face a grave issue. The inaccuracies in the identity verification by the technology could deprive some of these individuals of their recognition, effectively excluding them from the protections within the Canadian space, mirroring the exclusion and inequality perpetuated by Jim Crow laws. Moreover, the repercussions of this technological exclusion are long-lasting and severe. Incorrect identification that results in non-recognition could lead to deportation from Canada, exposing individuals to risks to their life, liberty, and personal security[80] in places far from Canada, underscoring the enduring and profound impact of such exclusions.

B. Perpetuation of Discrimination

A critical parallel between FRT and the Jim Crow laws resides in their capacity to perpetuate discrimination, albeit through different mechanisms. The Jim Crow laws were explicitly crafted and implemented as systemic instruments for enforcing racial segregation and discrimination. FRT, while sophisticated and modern, serves as an inadvertent but potent tool for reinforcing racial bias and discrimination. This technology, through its algorithmic biases and flawed training data, subtly embeds discrimination and racism into its operations, affecting individuals based on their race, gender, and other identities. Cathy O'Neil rightly noted that racism in technology "is powered by haphazard data gathering and spurious correlations, reinforced by institutional inequities, and polluted by confirmation bias."[81]

---

den Uses Facial Recognition to Ban Its Owner's Enemies", *New York Times* (22 December 2022), online: <nytimes.com> [perma.cc/27TB-HR2E]).

80 *Charter*, *supra* note 17, s 7.

81 Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (New York: Crown Publishers, 2016) at 23.

While the Jim Crow laws were a manifest expression of state-sanctioned discrimination aimed at maintaining racial inequality, the biases inherent in FRT often stem from unintentional consequences related to technological design, development, and deployment. These biases are not the result of deliberate policy but rather emerge from a lack of diversity in training data, algorithmic bias, and the oversight of developers and engineers. The inadvertent nature of this discrimination, however, does not diminish the fact that both Jim Crow laws and biased facial recognition practices ultimately lead to the same end result—perpetuation of discrimination and systemic marginalization of certain racial groups.

C. Legal and Social Implications

Jim Crow laws, when they were enacted, became an integral part of the legal system, serving as exclusionary tools for enforcing discrimination and segregation. Their integration into the fabric of the society established a normative social order that carries both legal and social implications. Similarly, while FRT and its biases have not been explicitly codified into a legal framework in Canada, it is swiftly gaining a semblance of legal legitimacy through its often covert integration into government operations and public sectors, particularly in law enforcement.[82] This tacit endorsement is highly problematic, given the absence of a regulatory framework or adequate oversight to mitigate its racial biases. Indeed, it sets a kind of precedent, implying it is part of the normative legal and operational framework—despite its propensity for discriminatory outcomes like wrongful arrests and the revocation of refugee statuses for individuals from racial and gender groups where the technology has a higher propensity for bias.[83]

On the societal front, Jim Crow laws were normalized through social norms and attitudes that endorsed racial discrimination as part of the status quo, notwithstanding its inherent flaws. Similarly, FRT is slowly being accepted socially regardless of these same integral flaws.[84] This ac-

---

[82] See *Barre*, *supra* note 5 at para 46; *AB*, *supra* note 5 at para 37; *Abdulle*, *supra* note 5 at paras 25, 34.

[83] *Barre*, *supra* note 5 at para 46; see e.g. *supra* note 53.

[84] This is evident in the voluntary use of the technology in daily aspects of life, such as unlocking digital devices like cell phones and personal computers, and even sorting and tagging digital photos. As Jennifer Lynch, General Counsel for Electronic Frontier Front was quoted as saying, "The more we use face recognition, the less we start to think of it, the less we think of it as risky out in the world, we become accustomed to it [...] I think it's a slippery slope from using face recognition on your phone to the government using face recognition to track us wherever we go" (Thorin Klosowski, "Facial Recognition Is Everywhere. Here's What We Can Do About It", *Wirecutter, New York Times* (15 July 2020), online: <nytimes.com> [perma.cc/Q4FZ-LA9]).

ceptance is partly due to the widespread but erroneous belief in technology's neutrality and objectivity. Selinger and Rhee's concept of normalization clearly demonstrates this phenomenon. They used the term "favourably disposed normalization" to depict a state in which surveillance becomes so commonplace that individuals not only accept it, but also rationalize it as beneficial.[85]

Sarah Hamid strongly opposed the social normalization of FRT, instead adopting an abolitionist stance.[86] She argued that FRT is inherently oppressive, and that using the technology, even for benevolent purposes, does not alter its nature as a tool of surveillance and control. Hamid went on to suggest that even individuals who use FRT for such benevolent purposes as unlocking their phones inadvertently contribute to the development and enhancement of this carceral technology, reinforcing its oppressive capabilities. Although Hamid's perspective might seem extreme, suffice to state that in a society largely unaware of the racial biases embedded in the technology, the purported convenience, efficiency, and public safety benefits of FRT can overshadow its inherent flaws, especially in a North American context marked by criminal profiling of individuals from racial groups and heightened fears of immigration.[87] Thus, while Jim Crow laws expressly legalized racism in the past, FRT is now normalizing it in contemporary society, often without society realizing it.

For many who perceive FRT as unbiased and objective, instances such as *Barre*, *AB*, *Abdulle*, and others may seem commendable, since immigration authorities utilize it to detect what may appear to be cases of immigration fraud.[88] However, this conception overlooks the significant risk of inaccuracies inherent in the technology, and the fact that individuals from certain racial groups are significantly affected by its predictive inac-

---

85 Evan Selinger & Hyo Joo (Judy) Rhee, "Normalizing Surveillance" (2021) 22:1 Northern European J Philosophy 49 at 59.

86 Sarah Hamid, "Community Defense: Sarah T. Hamid on Abolishing Carceral Technologies", *Logic(s) Magazine* (31 August 2020), online: <logicmag.io> [perma.cc/65H9-48B2].

87 Calvin D Lawrence, an African American engineer at IBM, admitted, "I did help design and develop several policing applications that were used to identify suspects using technologies like facial recognition. But, of course, I didn't consider that a racist and misguided cop could use it in a nefarious way" (Lawrence, *supra* note 2 at xii). He expressed further regret, "I'm both embarrassed and remorseful to admit that I didn't even consider how facial recognition systems could serve as a tool to harm communities of colour" (*ibid* at 68).

88 *Barre*, *supra* note 5 at paras 1–2; *AB*, *supra* note 5 at para 1; *Abdulle*, *supra* note 5 at para 1.

curacy. Like Calvin D. Lawrence noted, "[w]hen [AI] tech goes wrong, it often goes terribly for people of color."[89]

Jim Crow laws were intentionally crafted to undermine the achievements Black people in America attained during Reconstruction, the period following the American Civil War in the 19th century. These accomplishments ignited a civil rights movement in North America that played a crucial role in dismantling Jim Crow's racism.[90] Today, contemporary AI technologies, such as FRT, are subtly and unintentionally reincarnating the discriminatory practices of the past. These technologies risk undoing the progress made by the Civil Rights Movement, working in a similarly insidious manner to how the Jim Crow laws functioned. Therefore, we face an urgent need for a new civil rights movement, one focused on technology, to safeguard the societal gains we have made as a society. This is a clarion call to action, urging us to recognize and combat the AI manifestations of systemic racism before they erode the foundations of equality and justice in our society.

Conclusion

We stand at a pivotal moment in the interplay between technology and race. The parallels drawn between the racial biases embedded in FRT and the systemic racism of the Jim Crow era highlight not just a technological issue but a profound and novel racial justice crisis. As has been seen through various examples and judicial litigation, the deployment of FRT in immigration processes risks perpetuating discriminatory practices that society has long struggled to overcome.

The cases of *Barre, AB, Abdulle*, and others underscore the need for transparency, accountability, and procedural fairness in the use of FRT by the Canadian immigration and border control authorities. The refusal to disclose the technological underpinnings of decision-making processes not only undermines trust in these institutions but also veils the potential for inherent biases within these systems. While this paper does not advocate for the complete abolition of FRT as suggested by Hamid, there remains a compelling challenge. The challenge lies in not only improving the accuracy of FRT across racial lines but also ensuring its application aligns with the principles of transparency, justice, and equality that form the bedrock of Canadian society. This approach could entail a moratorium

---

89 Lawrence, *supra* note 2 at xiv.

90 Alexander, *supra* note 3 at 38, 44.

on the use of this tool in vital immigration processes, like refugee status revocation, until these principles are enshrined in policy and practice.[91]

This research analysis illustrates the urgent need for a regulatory and ethical framework that addresses the complexities of using AI in sensitive societal domains. Such a framework must prioritize the protection of individual rights, particularly individuals from marginalized communities who are most at risk of being adversely impacted by biases in AI technologies. It calls for a concerted effort among technologists, policymakers, civil society, and affected communities to engage in a dialogue aimed at reimagining the role of AI technologies in society. This dialogue must be rooted in an understanding of historical injustices and a commitment to preventing the reemergence of Jim Crow in new digital forms.[92]

Furthermore, the discussion around FRT and systemic racism extends beyond the boundaries of immigration and touches on broader issues of surveillance, privacy, and social control. The normalization of surveillance technologies under the guise of security and efficiency poses significant questions about the kind of society we want to build and the values we wish to uphold. As Sarah Hamid's abolitionist stance suggests, the uncritical adoption of technologies like FRT risks entrenching carceral logics into the fabric of daily life, reinforcing rather than dismantling structures of oppression.[93]

The research concludes with a call for a technological civil rights movement. Such a movement would advocate for the ethical development and deployment of AI technologies, ensuring they serve to enhance human rights and equality rather than diminish them. It would also push for the right of individuals to challenge the decisions made by or with the assistance of AI technologies, thus upholding the principles of procedural fairness and transparency.

As we move forward, it is imperative that we critically examine the technologies we adopt and their impact on society. The lessons from the past must guide our path forward, ensuring that technological advance-

---

91 Unfortunately, the new draft legislation on AI in Canada, the *Artificial Intelligence and Data Act* (AIDA) in Bill C-27, does not extend to the government's use of AI. Furthermore, this legislation lacks specific provisions to address racial bias within AI technologies. For more details, see Letter from Gideon Christian to the House of Commons Standing Committee on Industry and Technology (1 March 2024), online: <ourcommons.ca> [perma.cc/46G2-DR2H].

92 See generally Benjamin, *supra* note 4.

93 Hamid, *supra* note 86. See also Safia Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York: New York University Press, 2018) at 1; Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (New York: St. Martin's Press, 2018).

ments contribute to a more just and equitable world. This pathway requires vigilance, advocacy, and a willingness to challenge the status quo, ensuring that the digital future we build is inclusive, equitable, and reflective of our highest aspirations as a society.[94]

---

[94] After completing work on this paper and during its final review for publication, the CBSA developed and deployed an AI facial recognition tool, ReportIn, to track individuals on Canada's deportation list by verifying their identity and recording their location. While this latest development is not discussed in the paper, readers may find additional insights in the author's blog on CBSA's use of the tool (see Gideon Christian, "CBSA Border Surveillance: The Dangerous Expansion of Facial Recognition Technology" (4 November 2024), online (blog): <cila.co> [perma.cc/Q4PQ-APKK]).